First Look

IBM Cloud Pak for Security: A Connected Security Platform for the Hybrid, Multi-cloud World

Date: December 2019 **Author:** Jack Poller, Senior Analyst

Security Analytics and Operations Challenges

41%
say the threat landscape is rapidly changing.

35%
collect and process more security data today.

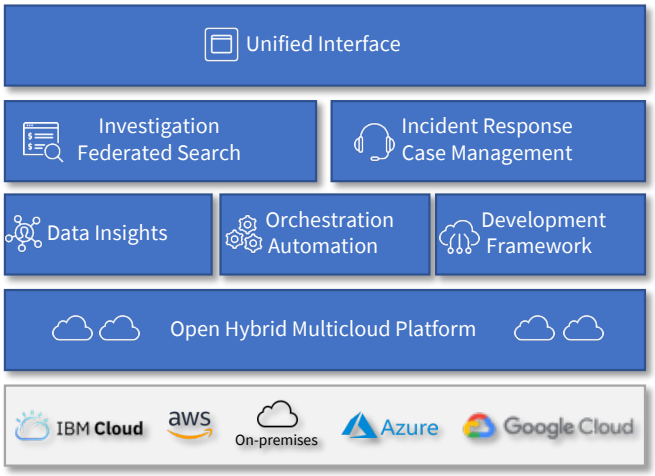
34%
say the volume of security alerts has increased.

Organizations are collecting and analyzing data from an ever-increasing range of telemetry including cloud, network, endpoint, and email controls. Using multiple security analytics and operations tools is de rigueur, with 77% deploying ten or more tools. Simultaneously, malicious actors are becoming more sophisticated, using multiple techniques to target specific organizations and individuals. Monitoring the expanding attack surface and managing an increasing number of alerts are two of the top challenges. These internal inefficiencies and fundamental external changes continue to make enterprise cybersecurity analytics and operations difficult.[1]

IBM Cloud Pak for Security

IBM designed Cloud Pak for Security to be an open platform where organizations can quickly integrate existing cybersecurity tools, generate deeper insights into threats, and orchestrate and automate responses while leaving telemetry data in place. With new open source technology to search and translate security data and foundational components of security orchestration, automation, and response (SOAR), IBM Cloud Pak for Security helps to operationalize data investigation, threat detection, and incident response.

IBM Cloud Pak For Security Architecture



Built on Red Hat OpenShift container technology, IBM Cloud Pak for Security is an open security platform that can run on-premises and in public clouds. The open ecosystem promotes tool interoperability, reducing vendor lock-in.

IBM's STIX-Shifter open source technology enables Cloud Pak for Security to connect to products that house security data repositories. The platform can analyze data resident in multiple disparate tools without having to first move the data to a central repository. This can improve the return on investment in cybersecurity tools and help organizations to gain security insights via investigation across data sets, leading to better risk-based decision making.

IBM Cloud Pak for Security connects cybersecurity tool workflows, reducing the time, effort, and expense of integrating tools and workflows, and enabling organizations to automate and orchestrate operations across security use cases. Incident response is accelerated, and organizations can extend the capabilities of their cybersecurity teams.

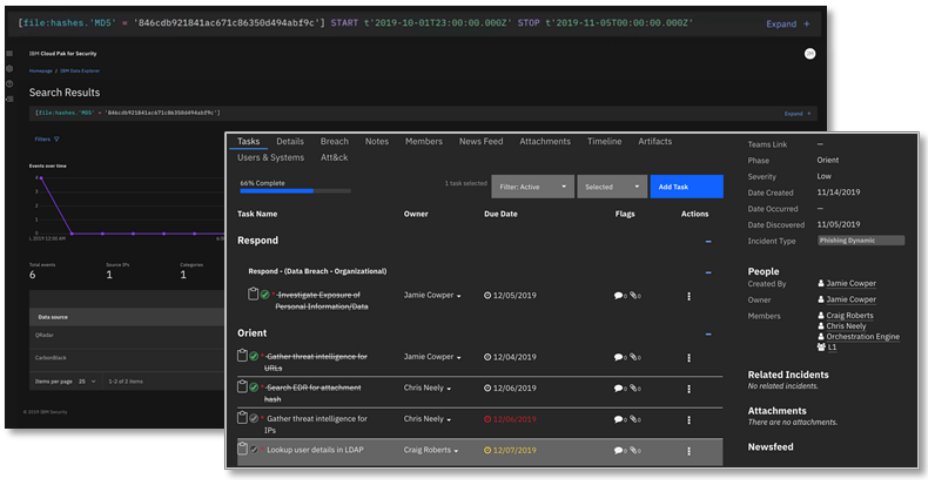
The first release of IBM Cloud Pak for Security incorporates two main features: federated search across data sets, providing threat investigation using a single integrated user interface, and incident response and case management.

[1] Source: ESG Research, *The Rise of Cloud-based Security Analytics and Operations Technologies*, August 2019.

ESG Demo Highlights

ESG evaluated the pre-release of IBM Cloud Pak for Security by leveraging a demo deployment managed through a standard web browser. The environment mimicked a typical enterprise IT infrastructure with a variety of endpoint, network, and cloud cybersecurity control systems. ESG followed the typical workflow of a security analyst investigating a threat.

Accelerating Time to Insight



- ESG started by reviewing a QRadar offense alert about a suspicious process.
- We pasted the process's MD5 hash into Data Explorer's STIX query builder. We specified time boundaries and selected data sources to be searched.
- While waiting for results, we reviewed previous queries, displayed as cards detailing the STIX query, data sources, and a sparkline with prior search results.
- When our query completed, we reviewed the results. We clicked on the IP address, which displayed enriched data, such as the host and users associated with that address.
- Next, we pivoted our search by clicking on *start a new query*, which brought up a new STIX query builder prepopulated with the search for the IP address.
- Refining our search further, we quickly uncovered that the suspicious process contained an unknown payload. We selected *create a case*, which automatically included the payload and created an incident response case.
- Next, ESG started the SOAR tool for IBM Cloud Pak for Security and clicked on the newly generated case.
- We noted that an automated incident-type specific playbook for the incident was generated, with tasks that guided the incident responder through the appropriate steps for each stage, starting with observe and orient.
- The security orchestration and automation tool filled in critical data from a variety of sources including threat intelligence feeds. As the automated steps proceeded, additional data was generated and added to the case.
- For incident resolution, security analysts can drive further remediation through integrations with a number of additional security and IT tools.

First Impressions

Organizations are challenged by the changing cyber-threat landscape and the growing IT attack surface driven by initiatives like cloud computing, digital transformation, and IoT. Concurrently, security operations centers (SOCs) struggle with disconnected point tools, manual processes, and a global cybersecurity skills shortage.

ESG's first look at the pre-release of IBM Cloud Pak for Security demonstrates the value of integrating cybersecurity tools into a single platform. Federated search across multiple disparate data sets accelerates cybersecurity analyst threat awareness and improves risk-based decision making without investing in moving data to a central repository. Integrated and connected workflows automate, orchestrate, and accelerate incident response, extending the cybersecurity team's breadth and depth of capabilities. Red Hat OpenShift improves Cloud Pak for Security ROI by enabling public and private cloud deployment and attendant containerization benefits such as increased reliability and uptime and decreased infrastructure management effort.